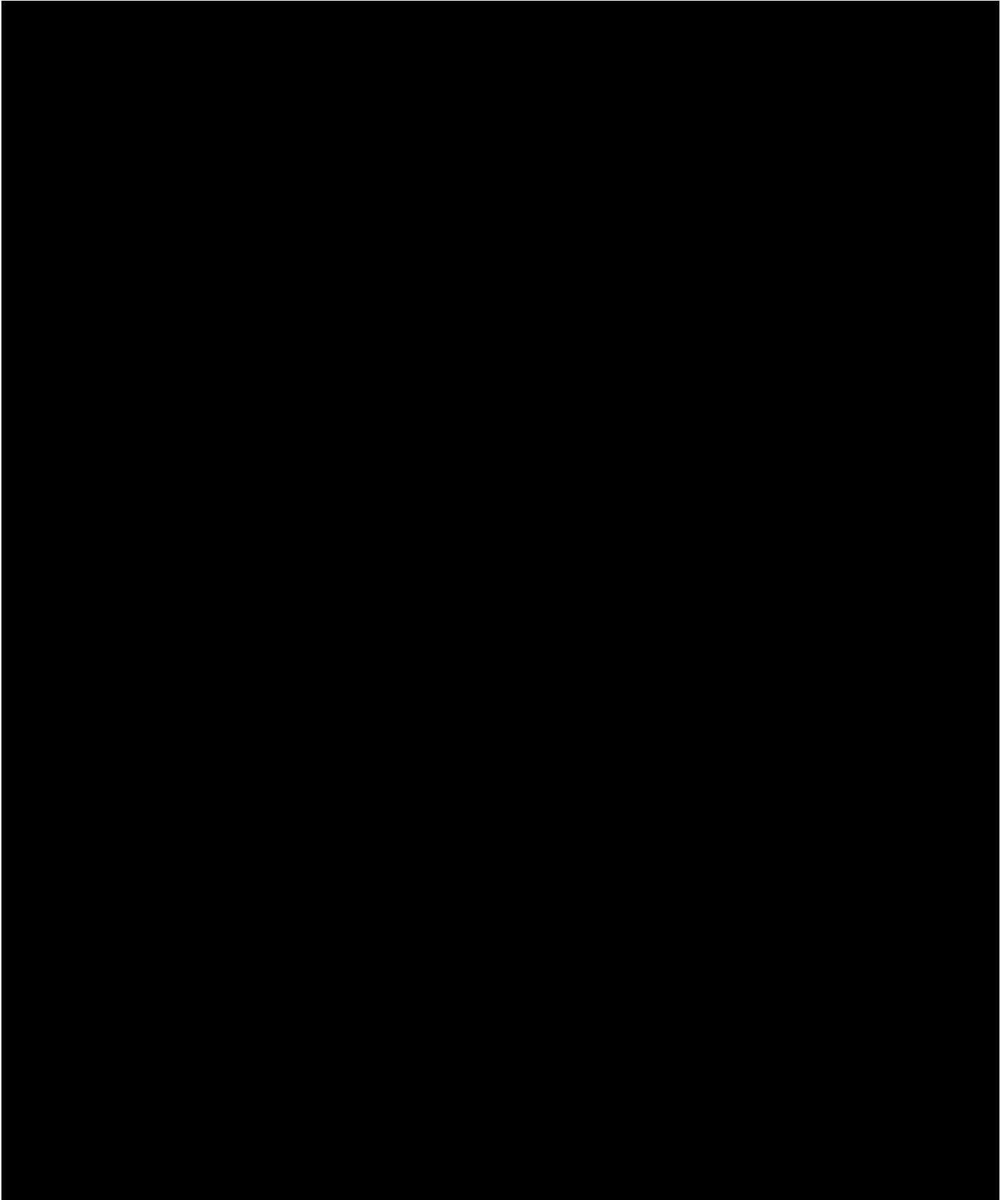


5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 841 (Possession with Intent to Distribute Cocaine) have been committed by [REDACTED] and [REDACTED] [REDACTED] in the Southern District of Alabama and elsewhere. There is also probable cause to search the information for evidence of these crimes, as described in Attachment A.



5

17. Many wireless phone providers generate and retain information about the location in which a particular communication was transmitted or received. Your affiant is aware, through training and experience, that when a cellular device is used to make or receive a call, or text message, or other communication, the wireless phone provider will maintain a record of which cell tower was used to process that contact. In general, but not always, the cellular telephone at issue will use the closest unobstructed tower that generates the strongest signal. These wireless providers maintain this information, including the corresponding cell towers (i.e., antenna towers covering specific geographic areas), “sectors” (i.e., faces of the towers), and other signaling data, as part of their regularly conducted business activities. Typically, a wireless provider maintains a record of the cell tower information associated with calls. These cell tower records are sometimes referred to as “cell site” data.

18. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law

20. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. Because the information is to be provided by T-Mobile and does not involve any physical intrusion by the government or any investigative agency, it is respectfully suggested that the normal time constraints requiring that the warrant be executed only in the daytime are not applicable.

24. Based on the foregoing, I submit that there is probable cause to conclude that that the cellular telephone having the number [REDACTED] was possessed by [REDACTED] while committing violation of 21 U.S.C. § 841 and was used to facilitate and coordinate that violation and that the requested information associated with the cellular telephone as further described herein and in Attachment A, is available from T-Mobile and that information, including cell site information,

RANDALL L
HOFFMAN

RANDALL L. HOFFMAN
Special Agent
Department of Homeland Security
Homeland Security Investigations (HSI)

P. Bradley Murray

HONORABLE P. BRADLEY MURRAY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number [REDACTED], (the “Account”) whose wireless service provider is T-Mobile USA, Inc. a company headquartered in New Jersey.
2. Records and information associated with the Target Cell Phone that is within the possession, custody, or control of T-Mobile USA, Inc. including information about the historical location of the cellular telephone and contents of communications, as further described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-Mobile

T-Mobile, USA Inc. is required to disclose the following records and other information, if available, to the United States for the cellular telephone having the number [REDACTED] which are stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider located in New Jersey (“Account”), for the time period May 1, 2023 to the present:

- A. The following information about the customers or subscribers of the Account:
1. Names (including subscriber names, user names, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 3. Local and long distance telephone connection records;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions; to include IP data session reports with associated cell site information;
 5. Length of service (including start date) and types of service utilized;
 6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”));
 7. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
 9. The content of communications, to the extent that they are available or were preserved.

- B. All records and other information (including the contents of communications) relating to the Account, including:
1. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 2. All data about which “cell towers” (i.e., antenna towers covering specific geographic areas), “sectors” (i.e., faces of the towers), and (if available) “azimuth” received a radio signal from each cellular telephone or device assigned to the Account; and
 3. RTT records, PCMD records, NELOS records, Timing Advance records, TrueCall records, MDT GPS records, and all other records containing timing advance measurements and distance-to-tower measurements for all technologies (CDMA, GSM, UMTS, LTE, etc.); and
 4. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 21 U.S.C. § 841 (Possession with Intent to Distribute Cocaine) involving the user of the account since May 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The location of the user of the account at times relevant to the investigation.
- (b) The content of user or owner's communications that may be evidence of the alleged crime;
- (c) The content of communications concerning the account user or owner's efforts to conceal the crime;
- (d) The identity of the person(s) who created or used the account or identifier, including records that help reveal the whereabouts of such person(s).
- (e) The identity of witnesses and/or co-conspirators with whom the account user communicated.